



UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

09/291,294 04/14/99 PALTEENGHE

C CITI0131-US

TM02/0129

EXAMINER

GEORGE T MARCOU  
KILPATRICK STOCKTON LLP  
700 13TH STREET N W SUITE 800  
WASHINGTON DC 20005

NORMAN, M

ART UNIT PAPER NUMBER

2163

DATE MAILED:

01/29/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/291,294	PALTENGHE ET AL.
	Examiner	Art Unit
	Marc E. Norman	2163

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### **Status**

1)  Responsive to communication(s) filed on 14 April 1999.

2a)  This action is **FINAL**.                    2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## **Disposition of Claims**

4)  Claim(s) 1-92 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5)  Claim(s) \_\_\_\_\_ is/are allowed.

6)  Claim(s) 1-12, 14-36, 41-42, 44-56, 62, 67, and 72-92 is/are rejected.

7)  Claim(s) 13, 37-40, 43, 57-61, 63-66, and 68-71 is/are objected to.

8)  Claims \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on 14 April 1999 is/are objected to by the Examiner.

11)  The proposed drawing correction filed on \_\_\_\_\_ is: a)  approved b)  disapproved.

12)  The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).  
a)  All b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

\* See the attached detailed Office action for a list of the certified copies not received.

14)  Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

**Attachment(s)**

15)  Notice of References Cited (PTO-892) 18)  Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_  
16)  Notice of Draftsperson's Patent Drawing Review (PTO-948) 19)  Notice of Informal Patent Application (PTO-152)  
17)  Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5. 20)  Other: \_\_\_\_\_

**DETAILED ACTION**

***Drawings***

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "46" has been used to designate both Trusted Third Party's Access (Figure 4) and Virtual Archivist (Figure 6). Correction is required.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 78 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 78 recites the limitation "wherein automatically updating the technology aspects further comprises" in lines 1-2 of the claim. There is insufficient antecedent basis for this limitation in the claim. Examiner has nevertheless examined below on the merits the limitations set forth in the claim.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-12, 14-36, 41-42, 44-56, 62, 67, and 72-92 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of official notice taken by the examiner and further in view of Rosen.

As per claims 1 and 81, Fischer teaches a method (and means therefor) of securely storing data (see column 2, lines 22-27) for an owner comprising storing the data (see column 1, lines 18-20), assigning a secret device (password) for the owner to access the stored data (see lines 45-47), automatically escrowing the information (see column 1, lines 42-45), and receiving personal verification from the user to access the stored data (see column 3, lines 1-21). Fischer does not specifically teach the escrowing of the secret device being conditioned on the occurrence of an event (other than the loss of a password). However, official notice is taken by the examiner that method described is a process that is routinely performed by a bank with regard to safety deposit boxes (see for example page 9 of Public Legal Education Society of Nova Scotia regarding "Getting into a safety deposit box"). The bank securely stores data (e.g., important documents or computer diskettes) within the safety deposit box; assigns a secret device (a lock and key to the box) to the owner for accessing the data; escrows the secret device (i.e., keeps a copy of the key) conditioned on an event (such as the death of the owner); receives verification of the occurrence of the event (affidavit/death certificate); and accesses the data with the safety deposit key. Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to condition the escrow the secret device conditioned on an event whereby the data could be accessed using the escrowed secret device for the purpose of accessing the data in the event of the death of the owner. Furthermore, while the steps of this

safety deposit box process are not “automatically” performed, given the increasing electronification of the banking industry as exemplified by Rosen, it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the steps outlined above within context of an automated electronic banking system (i.e., wherein the data, secret device, and verification process are all electronic) for the purpose of automatically accessing securely stored electronic data upon an event such as the death of the owner.

As per claim 2, Figure 3 of Rosen teaches data stored on an electronic (virtual) wallet (see also Gunnerson regarding an overview of virtual wallets and De Rooij et al. regarding securely storing and retrieving data using an electronic wallet). Since the virtual wallet is simply another means for storing and handling data, it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the methods discussed above regarding claim 1 to data stored on a virtual wallet for the purpose of protecting and accessing the data on the virtual wallet.

As per claims 3-5, Figure 1 of Fischer further teaches a terminal (B, N) for entering data, the terminal being coupled to a server (main processor 2), and the terminal comprising a personal computer (see column 4, lines 56-57), respectively.

As per claim 6, Fischer teaches the server comprising the server of a trusted third party (escrow agent of Figure 1).

As per claims 7-8, Rosen further teaches a monetary system wherein the server (mainframe) comprises the server of a financial institution/bank (see column 10, lines 1-7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to

apply the data storage system (as discussed above with regard to claim 1) within the context of a financial institution/bank for the purpose of securely storing financially related data.

As per claim 9, Figure 1 of Fischer teaches the terminal being coupled to the server over a network (communications channel 12).

As per claims 10-12, official notice is taken that private networks, public networks, and the internet are all common network structures that would have been obvious for the purpose of electronically connecting a terminal to a server.

As per claim 14, official notice is taken that a function for updating of technology aspects (such as encryption technologies) of databases (as is performed by the virtual archivist function) is well known in the art (see Van Hoff et al., for an example), and would have been obvious to apply to a system using a virtual wallet for the purpose of keeping such a system up to date with the state of the art.

As per claims 15-17, see the discussions above of claims 3, 5 and 4, respectively.

As per claim 18, Figure 1 of Rosen teaches money module (virtual wallet) application 6 residing on a network server.

As per claim 19, Figure 1 of Rosen teaches transaction money module (virtual wallet) application 4 residing on the terminal.

As per claims 20 and 48, Fischer teaches storing “bank account number, safety deposit identifying indicia, vault combination...” (column 2, lines 25-26). Applying this to a virtual wallet application would have been obvious for the reasons set forth above regarding claim 2.

As per claim 21, official notice is taken that it would have been obvious to assign the secret device using a virtual wallet application for the reasons set forth above regarding claim 2.

As per claim 22, Fischer teaches assigning the secret device to the owner at a terminal (terminal's B, N of Figure 1).

As per claim 23, Fischer teaches server (main processor) 2 assigning the secret key (held in secret private key store 5) and the server being coupled to the terminal via communications channel 12. Applying this to a virtual wallet application would have been obvious for the reasons set forth above regarding claim 2.

As per claims 24-27, see the discussions above regarding claims 5-8, respectively.

As per claim 28, Fischer teaches automatically sending information about the secret device to terminal (B, N of Figure 1) coupled to the server 2 over network (communications channel) 12. (See column 6, lines 34-37).

As per claims 29-31, see the discussions above regarding claims 10-12, respectively.

As per claims 32-33, Fischer further teaches escrowed digital secrets having at least two access aspects: an owner's access aspect (user password) and a trusted third party (trustee) aspect (See column 2, lines Abstract, lines 25-29: "The trustee utilizes documentary evidence presented by the alleged legitimate user and determines whether such evidence matches with the previously encrypted escrow information stored in the escrow record created by the user.")

As per claim 34, official notice is taken that it is common practice for a user to be sent a password (access aspect) for access to secured information. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the user be provided the password of Fischer for the purpose facilitating the security process.

As per claim 35, Fischer further teaches storing the trusted third party's access aspect (see, for example, column 2, lines 27-31).

As per claim 36, see discussion above regarding claim 2.

As per claim 41, Fischer teaches escrowing the trusted third-party's access aspect (see column 2, lines 45-47).

As per claim 42, see discussion above regarding claim 2.

As per claim 44, see discussion above of claim 1 regarding storing the access aspect being conditioned on the occurrence of an event.

As per claims 45-46, official notice is taken that, based on the analogy of the safety deposit box presented regarding claim 1, owners death or incompetence would be obvious events upon which to condition access to the third party's access aspect.

As per claim 47, Fischer teaches automatically escrowing secret access information (password) for the owner (see column 2, lines 19-31).

As per claim 49, Fischer teaches escrowing decryption infrastructure for the owner (see column 2, lines 20-22 regarding escrowing a symmetric DES encryption/decryption key).

As per claim 50, official notice is taken that these are all common and well known methods of decryption (such as referred to by Fischer in column 1, lines 25-28) that would have been obvious to one of ordinary skill in the art for the purpose of accessing the stored information.

As per claims 51-55, official notice is taken, based on the analogy of the safety deposit box presented regarding claim 1, that verification by a trusted third party, verification by a personal representative of the owner, verification of an event affecting the owner, and the event being either the owner's death or incompetence, would have been obvious to one of ordinary skill in the art at the time the invention was made.

As per claims 56 and 62, see the discussion above of claim 2 regarding the use of a virtual wallet.

As per claim 67, Fischer teaches accessing data using a trusted third party's (escrow agent of Figure 1) access aspect (see column 3, lines 31-34).

As per claims 72 and 78, official notice is taken that automatically updating of technology aspects (such as encryption technologies) of databases is well known in the art (see Van Hoff et al., for an example), and would have been obvious to apply to the system of Fischer for the purpose of keeping the system up to date with the state of the art.

As per claim 73, official notice is taken that a function for automatically updating of technology aspects (such as encryption technologies) of databases (as is performed by the virtual archivist function) is well known in the art (see Van Hoff et al., for an example), and would have been obvious to apply to a system using a virtual wallet for the purpose of keeping such a system up to date with the state of the art.

As per claims 74-77, see the discussions above of claims 4, 6, 7, and 8 regarding servers, trusted third parties, financial institutions, and banks, respectively.

As per claim 79, Fischer teaches receiving data from a third party (escrow agent). See the discussion above of 2 regarding the use of a virtual wallet.

As per claim 80, Fischer teaches the transfer of data via electronic messages. Again see the discussion above of 2 regarding the use of a virtual wallet.

As per claims 82, 84, 86, 88, 89, and 91, see discussion above of claim 4 regarding Rosen teaching a terminal coupled to a server.

As per claims 83, 87, 90, and 92, see discussion above of claim 6 regarding Rosen teaching the server of a trusted third party.

As per claim 85, Figure 3 of Rosen teaches the terminal being coupled to the server over a network.

#### *Allowable Subject Matter*

Claims 13, 37-40, 43, 57-61, 63-66, and 68-71 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The prior art neither teaches nor suggests the limitation regarding a virtual executor function of an electronic wallet application.

#### *Conclusion*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sudia teaches a cryptographic system and method with a key escrow feature and using a trusted third party.

De Rooij et al. teaches a method of securely storing and retrieving monetary data. Public Legal Education Society of Nova Scotia teaches information for executors regarding accessing a safety deposit box.

Perry provides an introduction to the use of virtual wallets.

Baldwin et al. teaches cryptographic techniques for electronic transactions.

Gunnerson teaches an overview of currently available virtual wallets.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Marc E. Norman whose telephone number is 703-305-2711.

MN  
January 18, 2001



TARIQ R. HAFIZ  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100